

Application No.: 09/381,996
Amendment Dated: January 23, 2007
Reply to Office Action: August 23, 2006

MTS-V03175

Amendments to the Drawings:

The attached sheet of drawings includes changes to Figures 27(a) and 27(b). This sheet replaces the original sheet(s).

Attachment

Application No.: 09/381,996
Amendment Dated: January 23, 2007
Reply to Office Action: August 23, 2006

MTS-V03175

Remarks/Arguments:

Applicants' disclosure is directed to a data recording and reproducing apparatus and method. Using Applicants' apparatus and method, digital data is encrypted using a contents key. The contents key itself is then encrypted using one of a plurality of key-encrypting keys. The encrypted digital data and the encrypted contents key are then recorded and reproduced.

Claim 39 stands rejected under 35 U.S.C. § 103(a) as being anticipated by Tsukamoto et al. (U.S. Patent Number 5,796,828) in view of Kori (U.S. Pub. No. 2001/0053979) and further in view of Aizawa (U.S. Patent Number 5,646,993). It is respectfully submitted, however, that the claims are patentable over the art of record for the reasons set forth below.

Tsukamoto is directed to an apparatus and method for transferring from a broadcaster to a receiver a limited reproduction right in data. In relevant part, Kori discloses a receiving system that receives, descrambles and encrypts digital video signals.

Kori is directed to a method and apparatus for protecting copyrighted digital data. In relevant part, Kori discloses encrypting data using a data encrypting key. The data encrypting key itself is then encrypted using a user management key.

Aizawa is directed to an information reproducing method and apparatus having a data protecting function. In relevant part, Aizawa discloses encrypting data using an encryption key. The encrypted data and the encryption key are then recorded on an optical disk. Finally, an information erasing unit erases the encryption key.

Applicants' invention, as recited by claim 39, includes features which are neither disclosed nor suggested by the art of record, namely:

...a key-encrypting key generating means for generating a plurality of key-encrypting keys...each of said plurality of key-encrypted keys is different from each other...

...a storing means...for deleting or making invalid each of said key-encrypting keys in sequence ...

...a key encrypting means for generating encrypted contents key...by using one of the plurality of said key-encrypting keys...(emphasis added).

This means Applicants' apparatus is capable using a contents key to encrypt digital data. The apparatus also generates additional keys, each of which is different from each other, such that one of the additional keys is used to encrypt the contents key itself. The apparatus is also adapted to invalidate each of the keys in sequence.

Tsukamoto discloses, at column 4, lines 4-18, an encipherer 22 that uses an encryption key to encrypt descrambled video signals. However, Tsukamoto does not disclose using key-encryption keys. That is, Tsukamoto does not disclose using another key to encrypt the encryption key itself. Examiner does not argue that Tsukamoto discloses key-encryption keys.

Kori does disclose use of a key-encryption key. As provided in paragraphs 79-81 of Kori, Kori discloses using an encryption key to encrypt data. Then, using a user management key *ku*, the data encryption key itself is encrypted. However, Kori only discloses use of a data encryption key (see paragraph 80, line 3).

This is different because Applicants disclose generating a plurality of different key-encryption keys and using one of the plurality of key-encryption keys to encrypt the contents key. Kori, on the other hand, only discloses use of one key-encryption key. Thus, Kori does not disclose generating a plurality of different key-encryption keys and using one of the plurality of key-encryption keys to encrypt the content key, as required by Applicants' claim 39, as amended.

Aizawa discloses, at column 5, lines 12-16 and 47-50, erasing the encryption key 14. Encryption key 14, as described at column 3, lines 47-48 of Aizawa, is used to decode enciphered information. Thus, encryption key 14 is not a key-encrypting key as disclosed in Applicants' specification. Examiner nevertheless contends that it would be obvious to combine Aizawa with Kori and delete only the management key *ku* disclosed in Kori instead of deleting only the encryption key 14, as disclosed in Aizawa.

Application No.: 09/381,996
Amendment Dated: January 23, 2007
Reply to Office Action: August 23, 2006

MTS-V03175

Despite Examiner's argument, this is different because Kori does not disclose generating a plurality of key-encrypting keys. Thus, neither Kori, Aizawa, nor their combination, disclose deleting the plurality of key-encrypting keys in sequence. Because Kori only discloses use of one management key k_u for encrypting the data encryption key, there is no way Kori's one management key could be deleted in sequence.

It is because Applicants include the feature of ...a key-encrypting key generating means for generating a plurality of key-encrypting keys...each of said plurality of key-encrypted keys is different each other...a storing means...for deleting or making invalid each of said key-encrypting keys in sequence ...a key encrypting means for generating encrypted contents key...by using one of the plurality of said key-encrypting keys..., that the following advantages are achieved. Use of key-encrypting keys provides additional protection for the digital data (e.g. copyrighted data). Generating a plurality of key-encrypting keys and deleting them in sequence enables generating a new code, for example, each day and then deleting each once in sequence once it has been used for, for example, one week. Generating and deleting key-encrypting keys in this matter provides even more protection for the digital data.

Accordingly, for the reasons set forth above, claim 39 is patentable over the art of record.

Claims 4, 53 and 68, while not identical to claim 39, include features similar to claim 39. Accordingly, claims 4, 53 and 68 are also patentable over the art for the reasons set forth above.

Claims 5-28, 30-38 and 69 include all the features of claim 4 from which they depend; claims 40-45, 47-49 and 63-65 include all the features of claim 39 from which they depend; claims 54-57, 59 and 63-65 include all the features of claim 53 from which they depend. Thus, claims 5-28, 30-38, 40-45, 47-49, 54-57, 59, 63-65 and 69 are also patentable over the art of record for the reasons set forth above.

The specification and drawings have been amended in order to appropriately conform Applicants' specification to the drawings.

Application No.: 09/381,996
Amendment Dated: January 23, 2007
Reply to Office Action: August 23, 2006

MTS-V03175

In view of the amendments and arguments set forth above, the above-identified application is in condition for allowance which action is respectfully requested.

Respectfully submitted,


Lawrence E. Ashery, Reg. No. 34,515
Attorney for Applicants

LEA/DK/ds

Attachments: Figures 27(a) and 27(b) (1 sheet)

Dated: January 23, 2007

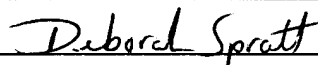
P.O. Box 980
Valley Forge, PA 19482
(610) 407-0700

The Director is hereby authorized to charge or credit Deposit Account No. **18-0350** for any additional fees, or any underpayment or credit for overpayment in connection herewith.

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail, with sufficient postage, in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on:

January 23, 2007

Deborah Spratt



ds/68169